日　本　国　特　許　庁
JAPAN　PATENT　OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:　２００２年１２月１９日

出願番号
Application Number:　特願２００２－３６７４６０

[ST.10/C]:　[ＪＰ２００２－３６７４６０]

出願人
Applicant(s):　株式会社メルコ

２００３年　１月２１日

特許庁長官
Commissioner,
Japan Patent Office　太田信一郎

出証番号　出証特２００２－３１０７６３０

【書類名】　特許願
【整理番号】　PA10F494
【提出日】　平成14年12月19日
【あて先】　特許庁長官　太田　信一郎　殿
【国際特許分類】　H04L 12/00
【発明者】
　【住所又は居所】　名古屋市南区柴田本通４丁目１５番　株式会社メルコ
　ハイテクセンター内
　【氏名】　石徹白　敬
【特許出願人】
　【識別番号】　390040187
　【氏名又は名称】　株式会社メルコ
【代理人】
　【識別番号】　110000028
　【氏名又は名称】　特許業務法人　明成国際特許事務所
　【代表者】　下出　隆史
　【電話番号】　052-218-5061
【手数料の表示】
　【予納台帳番号】　133917
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　0108819
【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　暗号鍵設定システム、アクセスポイント、および、暗号鍵設定方法、認証コード設定システム

【特許請求の範囲】

【請求項１】　無線ＬＡＮ用の中継器であるアクセスポイントと無線ＬＡＮ接続用デバイスを備えた端末との間で無線で通信される無線通信データを通信に先立って暗号化する際に用いられる暗号鍵を、前記端末に設定する暗号鍵設定システムであって、

前記アクセスポイントと前記端末との間の無線通信範囲を通常の通信範囲よりも狭める通信範囲限定手段と、

該通信範囲限定手段により無線通信範囲が狭められたとき、該通信範囲内に存在する端末と該アクセスポイントとの間で、前記暗号鍵の内容を表わす暗号鍵データを無線で通信することにより前記暗号鍵を設定する暗号鍵設定手段と

を備えた暗号鍵設定システム。

【請求項２】　請求項１に記載の暗号鍵設定システムであって、

前記アクセスポイントに対して前記暗号鍵の設定開始を指示する指示手段と、

該指示手段により指示に基づいて前記無線通信範囲を通常の通信範囲よりも狭める条件を決定する条件決定手段と

を備え、

前記通信範囲限定手段は、該条件決定手段により決定された条件下で、前記無線通信範囲を狭める手段である

暗号鍵設定システム。

【請求項３】　請求項１または２に記載の暗号鍵設定システムであって、

前記通信範囲限定手段は、前記アクセスポイントが、

前記端末から暗号鍵を設定する旨の指示を受信する際に、無線通信範囲を通常の通信範囲よりも狭める制御を行ない、

前記無線設定手段による暗号鍵の設定が終了したときに、無線通信範囲を通常の通信範囲に戻す制御を行なうことによって実現される

暗号鍵設定システム。

【請求項４】　前記通信範囲限定手段は、前記アクセスポイントの送信出力を調整することにより前記無線通信範囲を狭める手段である請求項１ないし３のいずれかに記載の暗号鍵設定システム。

【請求項５】　前記通信範囲限定手段は、前記暗号鍵の設定が行なわれる端末およびアクセスポイントを前記無線信号に対して遮蔽する遮蔽体である請求項１に記載の暗号鍵設定システム。

【請求項６】　前記アクセスポイントは、通信対象となる端末に固有の情報を登録する登録手段を備えた請求項１ないし５のいずれかに記載の暗号鍵設定システム。

【請求項７】　無線ＬＡＮ接続用デバイスを備えた端末との間で無線での通信を行なう無線ＬＡＮ用の中継器であって、前記端末との無線での通信に先立って、設定された暗号鍵を用いて通信対象となる無線通信データを暗号化し、該暗号化された無線通信データを用いて前記端末との無線通信を行なうアクセスポイントであって、

前記端末との間の無線通信範囲を通常の通信範囲よりも狭める通信範囲限定手段と、

該通信範囲限定手段により無線通信範囲が狭められたとき、該通信範囲内に存在する端末との間で、前記暗号鍵の内容を表わす暗号鍵データを無線で通信することにより前記暗号鍵を設定する暗号鍵設定手段と

を備えたアクセスポイント。

【請求項８】　無線ＬＡＮ用の中継器であるアクセスポイントと無線ＬＡＮ接続用デバイスを備えた端末との間で無線で通信される無線通信データを通信に先立って暗号化する際に用いられる暗号鍵を、前記端末に設定する方法であって、

前記アクセスポイントと前記端末との間の無線通信範囲を通常の通信範囲よりも狭め、

該無線通信範囲が狭められたとき、該通信範囲内に存在する端末と該アクセスポイントとの間で、前記暗号鍵の内容を表わす暗号鍵データを無線で通信することにより前記暗号鍵を設定する

暗号鍵設定方法。

【請求項９】　無線ＬＡＮ接続用デバイスを備えた端末が無線ＬＡＮ用の中継器であるアクセスポイントに無線で通信してネットワーク上の所定のデータにアクセスする際に要求される認証コードを、前記端末および前記アクセスポイントのうちの少なくとも一方に設定する認証コード設定システムであって、

前記アクセスポイントと前記端末との間の無線通信範囲を通常の通信範囲よりも狭める範囲限定手段と、

該通信範囲限定手段により無線通信範囲が狭められたとき、該通信範囲内に存在する端末と該アクセスポイントとの間で、前記認証コードの内容を表わすデータを無線で通信することにより前記認証コードを設定する設定手段と

を備えた認証コード設定システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、無線ＬＡＮ用の中継器であるアクセスポイントと無線ＬＡＮ接続用デバイスを備えた端末との間で無線で通信される無線通信データを通信に先立って暗号化する際に用いられる暗号鍵を、前記端末および前記アクセスポイントに設定する技術に関する。

【０００２】

【従来の技術】

近年、無線ＬＡＮ用の中継器であるアクセスポイントは、離れた位置にある複数のコンピュータをインターネットに接続するデバイスとして、自宅やオフィス内等の特定人が継続的に活動する場所（以下、プライベートスペースという）のみならず、ホテルや空港，商店街，公園，駅等の不特定多数の人が一時的に活動する場所（以下、パブリックスペースという）でも利用され始めている。例えば、アクセスポイントを、ｘＤＳＬ回線やＣＡＴＶ回線等の高速なインターネット接続サービスを実現するブロードバンド回線に接続してパブリックスペースに配置することにより、アクセスポイントから発信された電波が届く範囲（無線通信エリア）内にいる不特定多数人に対して自由にインターネットに接続できる空間

（以下、フリースポットという）を提供するサービスが提案されている。即ち、パブリックスペースの管理者が加入しているブロードバンド回線を、無線ＬＡＮ用のアクセスポイントを用いてパブリックスペースの利用者が所持する端末に開放するのである。これにより、利用者によるインターネット接続の利便性が高まり、パブリックスペースの利用促進を図ることができる。

【０００３】

このようなフリースポットでは、無線通信エリア内での無線ＬＡＮを介したインターネットへの接続権限を、限定者（例えば、お得意様）のみに認める場合があり、こうした場合には、限定者以外の人によるネットワークへの不正侵入を防止する必要があった。また、多数の人が集まるフリースポットでは、各人が所持する端末とアクセスポイントとの間で無線通信用の電波が頻繁に飛び交うので、多数の各人のプライバシーを十全に保護するために、無線通信エリア内での電波の傍受により通信内容が第三者に漏洩することを確実に防止する必要があった。

【０００４】

一方、無線ＬＡＮに関しては、従来、ネットワークへの不正侵入や通信内容の第三者への漏洩を防止するセキュリティ技術が種々提案されていた。例えば、端末に装着される無線ＬＡＮ接続用デバイス（例えば、無線ＬＡＮアダプタ）に予め割り当てられた固有の識別番号であるＭＡＣ（Ｍｅｄｉａ　Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌ）アドレスを利用し、このＭＡＣアドレスをアクセスポイントに登録しておき、端末からのアクセスに伴ってアクセスポイントがＭＡＣアドレスの認証を行ない、登録されたＭＡＣアドレス以外のＭＡＣアドレスであれば、該端末からのネットワークへの接続要求を拒否する技術（以下、ＭＡＣアドレス制限という）が提案されていた（例えば、特許文献１を参照）。また、端末およびアクセスポイントに、共通の暗号鍵としてＷＥＰ（Ｗｉｒｅｄ　Ｅｑｕｉｖａｌｅｎｔ　Ｐｒｉｖａｃｙ）キーを設定しておき、端末とアクセスポイントとの間でやりとりされるデータの内容をＷＥＰキーを用いて暗号化し、データが漏洩した場合であっても、データの内容を解析しにくくし、データの内容がわからないようにする技術（以下、ＷＥＰ暗号化という）も提案されていた（例えば、特許文献２を参照）。

【０００５】

【特許文献１】

特開２００１－３２０３７３号公報

【特許文献２】

特開２００１－３４５８１９公報

【０００６】

よって、セキュリティが確保されたフリースポットを実現するためには、フリースポットの利用に先立って、フリースポットを利用しようとする各人の端末について、ＭＡＣアドレスの登録やＷＥＰキーの設定を行なっておく必要があった。

【０００７】

【発明が解決しようとする課題】

しかしながら、上記した従来のセキュリティ技術では、アクセスポイントへのＭＡＣアドレスの登録や端末へのＷＥＰキーの設定を手作業で行なわなければならず、無線ＬＡＮを利用する端末を新たに追加しようとする場合に煩雑かつ不便であるという課題があった。特に、パブリックスペースに設けられるフリースポットでは、フリースポットを利用しようとする者が多数存在し、しかも徐々に増えていく。このような多数の各端末所有者に、フリースポットを利用する条件として、ＭＡＣアドレスの登録やのＷＥＰキーの設定に関する端末操作を課すことは、極めて不便であり、現実的でなかった。

【０００８】

また、端末側で任意の文字列を用いて設定されたＷＥＰキーをアクセスポイント側にも設定するためには、無線ＬＡＮを利用して設定すること、即ち、端末からＷＥＰキーのデータを電波に乗せてアクセスポイントに無線で送信し、これを受信したアクセスポイントが当該端末についてのＷＥＰキーを設定することが合理的である。こうすれば、端末所有者は、ＷＥＰキーの送信後すぐに、無線ＬＡＮを介した各種のサービス（例えば、インターネット接続）を利用することができるからである。このようにＷＥＰキーを無線で送信した場合には、端末とアクセスポイントとの間での電波の傍受によりＷＥＰキーが第三者に漏洩するおそれ

がある。この場合、漏洩したＷＥＰキーを手にした第三者は、ＷＥＰキーが設定された端末とアクセスポイントとの間でやり取りされる全てのデータを解析してデータの内容を知ることが可能となり、これでは暗号化によるセキュリティシステムが機能しなくなってしまう。特に、フリースポットのアクセスポイントでは、フリースポットを利用しようとする多数の者の端末についてＷＥＰキーの設定が行なわれるので、ＷＥＰキーの漏洩を十全に防止し、多数の各利用者の通信の秘密を十全に確保する必要がある。

【０００９】

そこで、本発明は、上記の課題を解決し、無線ＬＡＮを利用する端末の新規追加を、暗号鍵を表わすデータの漏洩を防止しつつ、簡便な手法で実現することを目的として、以下の構成を採った。

【００１０】

【課題を解決するための手段およびその作用・効果】

本発明の暗号鍵設定システムは、

無線ＬＡＮ用の中継器であるアクセスポイントと無線ＬＡＮ接続用デバイスを備えた端末との間で無線で通信される無線通信データを通信に先立って暗号化する際に用いられる暗号鍵を、前記端末に設定する暗号鍵設定システムであって、

前記アクセスポイントと前記端末との間の無線通信範囲を通常の通信範囲よりも狭める通信範囲限定手段と、

該通信範囲限定手段により無線通信範囲が狭められたとき、該通信範囲内に存在する端末と該アクセスポイントとの間で、前記暗号鍵の内容を表わす暗号鍵データを無線で通信することにより前記暗号鍵を設定する暗号鍵設定手段と

を備えたことを要旨とする。

【００１１】

上記の無線ＬＡＮ接続用デバイスは、端末とアクセスポイントとの間での無線通信を行なえるようにするために、端末に装着されるデバイスである。この無線ＬＡＮ接続用デバイスの一例として、無線ＬＡＮアダプタや無線ＬＡＮカードを考えることができる。

【００１２】

本発明の暗号鍵設定システムでは、アクセスポイントと端末との間で通信される無線通信データを暗号化する際に用いられる暗号鍵を設定する。こうした暗号鍵の設定は、アクセスポイントと端末との間の無線通信範囲が通常の通信範囲よりも狭められたとき、該端末と該アクセスポイントとの間で、暗号鍵の内容を表わす暗号鍵データを無線で通信することにより行なわれる。こうすれば、暗号鍵データを無線で通信した場合であっても、暗号鍵データはアクセスポイントを中心とした狭い範囲でやり取りされるので、暗号鍵データが乗った無線の傍受がしにくくなり、暗号鍵データの漏洩が防止される。従って、無線ＬＡＮを利用する端末の新規追加を、暗号鍵データの漏洩を防止しつつ、簡便に実現することが可能となり、加入し易い無線ＬＡＮを高いセキュリティレベルで実現することができる。

【００１３】

通信範囲限定手段を実現する態様として、種々の態様を考えることができる。例えば、アクセスポイント側で実現することも可能である。具体的には、アクセスポイントに対して前記暗号鍵の設定開始を指示する指示手段と、該指示手段により指示に基づいて前記無線通信範囲を通常の通信範囲よりも狭める条件を決定する条件決定手段とを備え、前記通信範囲限定手段を、該条件決定手段により決定された条件下で、前記無線通信範囲を狭める手段としてもよい。こうすれば、暗号鍵の設定開始が指示された場合に、この指示に基づいて決定された条件下で無線通信範囲が狭められ、暗号鍵の設定がなされる。従って、アクセスポイントを、常時、暗号鍵の設定を受け付ける状態にしておく必要がない。

【００１４】

アクセスポイントが、端末から暗号鍵を設定する旨の指示を受信する際に、無線通信範囲を通常の通信範囲よりも狭める制御を行ない、無線設定手段による暗号鍵の設定が終了したときに、無線通信範囲を通常の通信範囲に戻す制御を行なうこととしてもよい。こうすれば、端末の所有者は、暗号鍵の設定をアクセスポイントに触れることなく行なうことが可能となる。また、通信範囲限定手段を、アクセスポイントの送信出力を調整することにより前記無線通信範囲を狭める手段としてもよい。

【００１５】

通信範囲限定手段を、前記暗号鍵の設定が行なわれる端末およびアクセスポイントを前記無線信号に対して遮蔽する遮蔽体とすることも可能である。こうすれば、暗号鍵データが乗った無線（以下、暗号鍵無線という）が遮蔽体の外部に送出されたり、暗号鍵無線を傍受するための無線が遮蔽体の内部に侵入したりすることが確実に防止される。従って、暗号鍵データの第三者への漏洩を十全に防止することができる。

【００１６】

アクセスポイントが、通信対象となる端末に固有の情報を登録する登録手段を備えることとしてもよい。こうすれば、固有の情報が登録された端末についてのみ、無線ＬＡＮへの接続を許容することが可能となり、接続権限のない者による無線ＬＡＮへの接続を防止することができる。また、接続権限のない者がＬＡＮ上の端末やアクセスポイントに侵入して暗号鍵データ等の各種のデータを取得することを未然に防止することができる。

【００１７】

本発明のアクセスポイントは、

無線ＬＡＮ接続用デバイスを備えた端末との間で無線での通信を行なう無線ＬＡＮ用の中継器であって、前記端末との無線での通信に先立って、設定された暗号鍵を用いて通信対象となる無線通信データを暗号化し、該暗号化された無線通信データを用いて前記端末との無線通信を行なうアクセスポイントであって、

前記端末との間の無線通信範囲を通常の通信範囲よりも狭める通信範囲限定手段と、

該通信範囲限定手段により無線通信範囲が狭められたとき、該通信範囲内に存在する端末との間で、前記暗号鍵の内容を表わす暗号鍵データを無線で通信することにより前記暗号鍵を設定する暗号鍵設定手段と

を備えたことを要旨とする。

【００１８】

本発明のアクセスポイントでは、端末との間での通信対象となる無線通信データを暗号化する際に用いられる暗号鍵を無線で端末に通信し、端末に暗号鍵を設

定する。こうした暗号鍵の設定は、端末との間の無線通信範囲が通常の通信範囲よりも狭められたとき、該端末との間で、暗号鍵の内容を表わす暗号鍵データを無線で通信することにより行なわれる。こうすれば、暗号鍵データを無線で通信した場合であっても、暗号鍵データはアクセスポイントを中心とした狭い範囲でやり取りされるので、暗号鍵データが乗った無線の傍受がしにくくなり、暗号鍵データの漏洩が防止される。従って、無線ＬＡＮを利用する端末の新規追加を、暗号鍵データの漏洩を防止しつつ、簡便に実現することが可能となり、加入し易い無線ＬＡＮを高いセキュリティレベルで実現することができる。

【００１９】

本発明の暗号鍵設定方法は、

無線ＬＡＮ用の中継器であるアクセスポイントと無線ＬＡＮ接続用デバイスを備えた端末との間で無線で通信される無線通信データを通信に先立って暗号化する際に用いられる暗号鍵を、前記端末に設定する方法であって、

前記アクセスポイントと前記端末との間の無線通信範囲を通常の通信範囲よりも狭め、

該無線通信範囲が狭められたとき、該通信範囲内に存在する端末と該アクセスポイントとの間で、前記暗号鍵の内容を表わす暗号鍵データを無線で通信することにより前記暗号鍵を設定することを要旨とする。

【００２０】

本発明の暗号鍵設定方法では、アクセスポイントと端末との間で通信される無線通信データを暗号化する際に用いられる暗号鍵を端末に設定する。こうした暗号鍵の設定は、アクセスポイントと端末との間の無線通信範囲が通常の通信範囲よりも狭められたとき、該端末と該アクセスポイントとの間で、暗号鍵の内容を表わす暗号鍵データを無線で通信することにより行なわれる。こうすれば、暗号鍵データを無線で通信した場合であっても、暗号鍵データはアクセスポイントを中心とした狭い範囲でやり取りされるので、暗号鍵データが乗った無線の傍受がしにくくなり、暗号鍵データの漏洩が防止される。従って、無線ＬＡＮを利用する端末の新規追加を、暗号鍵データの漏洩を防止しつつ、簡便に実現することが可能となり、加入し易い無線ＬＡＮを高いセキュリティレベルで実現することが

できる。

【００２１】

本発明の認証コード設定システムは、

無線ＬＡＮ接続用デバイスを備えた端末が無線ＬＡＮ用の中継器であるアクセスポイントに無線で通信してネットワーク上の所定のデータにアクセスする際に要求される認証コードを、前記端末および前記アクセスポイントのうちの少なくとも一方に設定する認証コード設定システムであって、

前記アクセスポイントと前記端末との間の無線通信範囲を通常の通信範囲よりも狭める範囲限定手段と、

該通信範囲限定手段により無線通信範囲が狭められたとき、該通信範囲内に存在する端末と該アクセスポイントとの間で、前記認証コードの内容を表わすデータを無線で通信することにより前記認証コードを設定する設定手段と

を備えたことを要旨とする。

【００２２】

上記の認証コードとしては、アクセスポイントから有料情報を取得するために必要な個人情報（例えば、端末所有者の氏名，ＩＤやパスワード等）等を考えることができる。

【００２３】

本発明の認証コード設定システムでは、端末がアクセスポイントに無線で通信してネットワーク上の所定のデータにアクセスする際に要求される認証コードを、端末およびアクセスポイントのうちの少なくとも一方に設定する。こうした認証コードの設定は、アクセスポイントと端末との間の無線通信範囲が通常の通信範囲よりも狭められたとき、該端末と該アクセスポイントとの間で、認証コードの内容を表わすデータ（以下、認証コードデータという）を無線で通信することにより行なわれる。こうすれば、認証コードデータを無線で通信した場合であっても、認証コードデータはアクセスポイントを中心とした狭い範囲でやり取りされるので、認証コードデータが乗った無線の傍受がしにくくなり、認証コードデータの漏洩が防止される。従って、無線ＬＡＮを利用する端末に関する認証コードの設定を、認証コードデータの漏洩を防止しつつ、簡便に実現することが可能

となり、無線ＬＡＮのセキュリティレベルを高めることができる。

【００２４】

【発明の実施の形態】

以上説明した本発明の構成および作用を一層明らかにするために、以下本発明の実施の形態を、以下の順序で説明する。

Ａ．第１実施例（暗号鍵設定システムＬＨ１）

Ａ－１．暗号鍵設定システムＬＨ１の概要

Ａ－２．ＷＥＰキーの設定に関する処理の内容

Ａ－３．作用効果

Ｂ．第２実施例（暗号鍵設定システムＬＨ２）

Ｃ．変形例

【００２５】

Ａ．実施例：

Ａ－１．暗号鍵設定システムＬＨ１の概要：

図１は本発明の第１実施例である暗号鍵設定システムＬＨ１を実現するハードウェアの構成を示す説明図であり、図２はアクセスポイント２０の構成を示す説明図である。暗号鍵設定システムＬＨ１は、無線ＬＡＮの無線通信エリアＡＲ１内において、端末５０とアクセスポイント２０との間で、暗号鍵としてのＷＥＰキーの内容を表わすキーデータを電波に乗せて無線通信することにより、端末５０にアクセスポイント２０が使用するＷＥＰキーを設定するシステムである。

【００２６】

図１に示すように、無線通信エリアＡＲ１には、無線ＬＡＮ用の中継器であるアクセスポイント（無線基地局）２０が設置されている。アクセスポイント２０は、図２に示すように、ＣＰＵ１１と、このＣＰＵ１１とバスにより相互に接続されたＲＯＭ１２，ＲＡＭ１３，ハードディスク等の不揮発的な記憶装置１４，ネットワークインタフェースとしてのＷＡＮポート１７，有線ＬＡＮとの接続用のＬＡＮポート２２，無線通信インタフェース１８，ディスプレイコントローラ１５，入出力コントローラ１６等の各部を備える。

【００２７】

ＲＯＭ１２には、無線通信エリアＡＲ１内の端末５０，６０，７０との通信やインターネットＩＮへの接続に関する各種のプログラムとこのプログラムの実行に必要なデータが格納されている。入出力コントローラ１６にはプッシュ式の登録ボタン１２７が接続されている。登録ボタン１２７は、その押圧部がアクセスポイント２０の筐体表面に露出した状態で設けられている。ディスプレイコントローラ１５には、無線ＬＡＮの接続状態や通信状態を点灯・点滅等によって表示する各種の表示ランプ１９が接続されている。

【００２８】

無線通信インタフェース１８には、電波を送信する送信機２５，電波を受信する受信機２６が接続されている。この送信機２５，受信機２６は、外部への電波の送信や外部からの電波の受信が可能な状態で、アクセスポイント２０に内蔵されている。図１では、送信機２５の出力や受信機２６の受信感度を標準設定値とした場合に、送信機２５から送信された電波が届き、かつ、受信機２６が端末５０，６０，７０からの電波を受け取れる範囲を、無線通信エリアＡＲ１として表わしている。こうしたアクセスポイント２０の設置により、無線通信エリアＡＲ１内を通常の通信範囲とした無線ＬＡＮが組まれる。

【００２９】

なお、ＲＯＭ１２には、端末５０，６０，７０との通信に関するプログラムとして、送信機２５の出力の標準設定値を一時的に変更する処理の内容が記述された出力値変更プログラムや受信機２６の受信感度の標準設定値を一時的に変更する処理の内容が記述された受信感度値変更プログラムが予め格納されている。この設定値を変更する処理は、具体的には、標準設定値を１／ｎ（ｎは予め定められた定数）倍する演算処理によって実現される。ＣＰＵ１１は、この出力値変更プログラム，受信感度値変更プログラムを実行することにより、変更後の出力値や受信感度値を、無線通信インタフェース１８を介して送信機２５，受信機２６に出力する。これにより、送信機２５から送信される電波の出力や受信機２６における電波の受信感度が変更される。

【００３０】

端末５０，６０，７０は、周知のノート型のパーソナルコンピュータであり、

ＣＰＵ，ＲＯＭ，ＲＡＭ等からなる制御装置をはじめ、記憶装置としてのハードディスクやＣＤ－ＲＯＭドライブ等を備える。勿論、携帯情報端末（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔ）等の他の端末であっても差し支えない。

【００３１】

また、端末５０，６０，７０には、アクセスポイント２０との間での電波の送受信を行なえるようにする無線ＬＡＮ接続用デバイスとして、無線ＬＡＮアダプタ５２，６２，７２が装着されている。この無線ＬＡＮアダプタ５２，６２，７２のデバイスドライバが端末５０に組み込まれることにより、端末５０，６０，７０は、装着された無線ＬＡＮアダプタ５２，６２，７２を認識し、無線ＬＡＮアダプタ５２，６２，７２を制御することが可能となる。なお、無線ＬＡＮアダプタ５２，６２，７２には、アダプタに固有の識別番号であるＭＡＣアドレスが付与されている。

【００３２】

無線通信エリアＡＲ１内に入ったコンピュータとしての端末５０，６０，７０は、装着された無線ＬＡＮアダプタ５２，６２，７２とアクセスポイント２０との間で電波が送受信されることにより、アクセスポイント２０との通信を無線で行なう。アクセスポイント２０および無線ＬＡＮアダプタ５２，６２，７２は、やり取りするデータを通信に適した形式、いわゆるパケットに変換することが可能であり、これにより、端末５０，６０，７０とアクセスポイント２０との間において、オフライン（インターネットに接続されていない状態）でデータのやり取りをすることが理論上可能となる。

【００３３】

次に、アクセスポイント２０をインターネットＩＮに接続するための構成について説明する。図１に示すように、アクセスポイント２０のＷＡＮポート２４には、モデムを内蔵したルータ２８がケーブルを介して接続されている。ルータ２８は、無線ＬＡＮアダプタ５２，６２，７２それぞれのＭＡＣアドレスに基づいて、無線ＬＡＮ内の複数の各端末５０，６０，７０を特定し、これらを区別することができる。

【００３４】

ルータ２８内のモデムは、ＣＡＴＶ回線，ｘＤＳＬ回線等のブロードバンドな通信回線ＣＬ、プロバイダＰＶの専用回線を介してインターネットＩＮに接続されている。即ち、ルータ２８は、無線ＬＡＮをインターネットＩＮに接続するゲートウェイとして機能する。

【００３５】

なお、本実施例では、無線通信エリアＡＲ１内にいる者が所有する無線ＬＡＮアダプタを備えた端末のうち、ＭＡＣアドレスがアクセスポイント２０に登録されている端末（以下、登録端末という）に、無線ＬＡＮへの接続を許容する。登録端末の所有者は、自己の端末をアクセスポイント２０を通じてインターネットＩＮに接続し、インターネットＩＮ上のサーバＳＶに格納されたウェブコンテンツ等の種々の情報を取得することができる。一方、ＭＡＣアドレスがアクセスポイント２０に登録されていない端末（非登録端末という）は、たとえ無線通信エリアＡＲ１内にいても無線ＬＡＮに接続することができない。即ち、無線通信エリアＡＲ１は、登録端末の所有者のみにインターネットＩＮへの接続サービスを提供するフリースポットとされている。なお、図１では、端末５０，６０が登録端末に該当し、端末７０が非登録端末に該当するものとする。

【００３６】

こうした登録端末とアクセスポイント２０との間では、契約やサービス等の種々の内容を有するデータ（以下、内容付きデータという）が電波に乗せて送受信される。本実施例では、内容付きデータを送信する側の装置（登録端末，アクセスポイント２０）が、送信に先立って、既述したＷＥＰキーという暗号鍵を用いて内容付きデータを暗号化し、暗号化後の内容付きデータ（以下、暗号化データという）を受信側の装置（アクセスポイント２０，登録端末）に送信することとしている。受信側の装置は、受信した暗号化データをＷＥＰキーを用いて複号化し、内容付きデータを得るのである。

【００３７】

ＷＥＰは、ＩＥＥＥ８０２．１１で使用される、秘密鍵暗号方式（データの暗号化と暗号化されたデータの復号化の双方で同じ暗号鍵を使用する方式）の暗号

化技術であり、暗号鍵として６４ビットまたは１２８ビットのＷＥＰキーが用いられる。

【００３８】

こうしたＷＥＰキーを用いた暗号化により、無線通信エリアＡＲ１内において内容付きデータを乗せた電波が傍受された場合に、内容付きデータの解析がしにくくなり、通信内容の第三者への漏洩が防止される。例えば、登録端末からアクセスポイント２０にクレジットカードの番号を含む契約文書が送信された場合には、送信電波の傍受によりクレジットカードの番号が第三者に知られてしまうことを防止することができる。

【００３９】

Ａ－２．ＷＥＰキーの設定に関する処理の内容：

続いて、上記のＷＥＰキーを端末５０，６０に設定する手法について説明する。

【００４０】

アクセスポイント２０のＲＯＭ１２には、端末５０，６０との通信に関するプログラムとして、無線ＬＡＮアダプタ５２，６２のＭＡＣアドレスの登録に関するプログラム（ＭＡＣ登録プログラム）が予め格納されている。一方、無線ＬＡＮの使用に際して端末５０，６０にインストールされたユーティリティプログラムには、ＷＥＰキーの設定に関するプログラム（ＷＥＰキー設定プログラム）が含まれている。

【００４１】

上記のＷＥＰキー設定プログラムの内容を端末５０，６０のＣＰＵが実行し、このＷＥＰキー設定プログラムの実行に伴って上記のＭＡＣ登録プログラムおよび出力値変更プログラムの内容をアクセスポイント２０のＣＰＵ１１が実行することにより、図３に示すセキュリティデータ設定処理が行なわれる。このセキュリティデータ設定処理が行なわれることにより、アクセスポイント２０に無線ＬＡＮアダプタ５２，６２のＭＡＣアドレスが登録され、アクセスポイント２０および端末５０，６０に共通のＷＥＰキーが設定される。

【００４２】

セキュリティデータ設定処理の内容について図３ないし図４を説明する。図３はセキュリティデータ設定処理ルーチンを示すフローチャートである。図４は、出力値が変更された後の送信機２５における電波の送信可能範囲を、セキュリティ通信エリアＭＲ１として示す説明図である。この図３ないし図４に関する以下の説明では、ＭＡＣアドレスの登録対象ないしＷＥＰキーの設定対象となる端末が端末５０であると仮定して説明する。

【００４３】

セキュリティデータ設定処理ルーチンは、端末５０側のＣＰＵで実行されるルーチンＡとアクセスポイント２０側のＣＰＵ１１で実行されるルーチンＢとからなる。本ルーチンによる登録に先立ち、アクセスポイント２０の管理者は、端末５０がセキュリティ通信エリアＭＲ１内にあることを確認して登録ボタン１２７を作動させる（ステップＳ２００，Ｓ２１０）。セキュリティ通信エリアＭＲ１は、既述した出力値変更プログラムの実行によって標準設定値が一時的に低減された場合に、送信機２５による電波の送信が可能となる範囲である（図４を参照）。上記の登録ボタン１２７の作動により、アクセスポイント２０は、既述した出力値変更プログラムを実行して、送信機２５の出力値を標準設定値の１／ｎに低減する処理を行なう（ステップＳ２２０）。これにより、送信機２５が電波を送信できる範囲は、図４に示すセキュリティ通信エリアＭＲ１内となり、無線通信エリアＡＲ１よりも狭くなる。従って、無線通信エリアＡＲ１内に入っている登録端末であっても、セキュリティ通信エリアＭＲ１内に入っていない場合には、アクセスポイント２０にアクセスすることができなくなる。

【００４４】

次に、端末５０は、無線ＬＡＮアダプタ５２のＭＡＣアドレスを特定し、無線ＬＡＮに加入する旨の指示（以下、加入指示という）を表わすデータにＭＡＣアドレスをヘッダ情報として付加したパケットを、アクセスポイント２０に送信する処理を行なう（ステップＳ１００）。

【００４５】

続いて、受信したパケットのヘッダ情報からＭＡＣアドレスを読み取り、読み取ったＭＡＣアドレスをＲＡＭ１３のバッファ領域に一時的に記憶する処理を行

なう（ステップＳ２３０）。

【００４６】

続いて、使用するＷＥＰキーを表わすデータ（以下、ＷＥＰキーデータという）を端末５０に送信する処理を行ない（ステップＳ２５０）、ＷＥＰキーデータが端末５０に配信されたか否かを判断する処理を行なう（ステップＳ２５５）。この配信されたか否かの判断は、既述した無線ＬＡＮアダプタ５２のデータリターン機能を利用することにより実現することができる。ＷＥＰキーデータが端末５０に配信されていないと判断した場合には、ＲＡＭ１３に記憶されていたＭＡＣアドレスを消去し（ステップＳ２６０）、本ルーチンを終了する。

【００４７】

一方、ＷＥＰキーデータが端末５０に配信されたと判断した場合には、既述した出力値変更プログラムを実行して、送信機２５の出力値を標準設定値に戻す処理を行なう（ステップＳ２７０）。これにより、送信機２５が電波を送信できる範囲が、通常の範囲（無線通信エリアＡＲ１）となり、登録端末は、無線通信エリアＡＲ１内に入っていれば、アクセスポイント２０にアクセスすることができる。

【００４８】

続いて、端末５０のＭＡＣアドレスを、記憶装置１４の管理領域に登録する処理を行なう（ステップＳ２８０）。これにより、アクセスポイント２０側での端末５０に関するＭＡＣアドレスの登録が完了する。

【００４９】

一方、ステップＳ２５０の処理によってＷＥＰキーデータを受信した端末５０は、ＷＥＰキーをアクセスポイント２０のＩＰアドレスと関連付けて自動的に設定する処理を行ない（ステップＳ１１０）、本ルーチンを終了する。これにより、端末５０側でのアクセスポイント２０に関するＷＥＰキーの設定が完了する。以降、端末５０とアクセスポイント２０との間では、設定されたＷＥＰキーを用いて内容付きデータを暗号化した暗号化データが送受信される。

【００５０】

Ａ－３．作用効果：

以上説明した第１実施例の暗号鍵設定システムＬＨ１では、上記のセキュリティデータ設定処理を実行することにより、端末５０にＷＥＰキーを自動的に設定する。このような「ＷＥＰキーの無線通信による自動設定」がなされることで、無線ＬＡＮを利用する端末５０の新規追加を簡便に実現することが可能となり、加入し易い無線ＬＡＮを提供することができる。例えば、ＷＥＰキーの設定に際し、端末５０の所有者やアクセスポイント２０の管理者は、端末５０とアクセスポイント２０とをケーブル等で接続する必要がなく、また、ＷＥＰキーの作成や設定を手作業で行なう必要もない。特に、上記の暗号鍵設定システムＬＨ１をフリースポットに備えられた無線ＬＡＮに採用すれば、なお好適である。フリースポットの無線ＬＡＮは、これを利用しようとする多数の人が次々と新規に加入するものであり、各人の設定に伴って必要な作業を大きく軽減することができるからである。

【００５１】

更に、アクセスポイント２０は、ＷＥＰキーのデータを電波に乗せて端末５０に送信する際に、アクセスポイント２０から送信される電波が届く範囲を、通常の範囲である無線通信エリアＡＲ１から、より狭い範囲であるセキュリティ通信エリアＭＲ１に変更する。このため、ＷＥＰキーデータを乗せた電波が傍受される可能性が低くなる。例えば、図４において、アクセスポイント２０から端末５０にＷＥＰキーデータが送信された場合に、ＷＥＰキーデータを乗せた電波は、狭い範囲であるセキュリティ通信エリアＭＲ１内にしか届かず（矢印Ｑ１を参照）、セキュリティ通信エリアＭＲ１外にいる登録端末６０や非登録端末７０に受信されてしまうことがない。従って、上記のようにＷＥＰキーデータが無線で送信される場合であっても、ＷＥＰキーの漏洩を防止することが可能となり、セキュリティレベルの高い無線ＬＡＮを実現することができる。特に、このようなアクセスポイント２０をフリースポットに設置した場合には、フリースポットを利用しようとする多数の者の端末について、ＷＥＰキーの設定時にＷＥＰキーが第三者に漏洩してしまうことが確実に防止される。従って、多数の各利用者の通信の秘密を十全に確保することができる。

【００５２】

また、第１実施例の暗号鍵設定システムＬＨ１では、アクセスポイント２０は、端末５０からの加入指示を表わすデータの受信に伴って一時的に通信範囲を狭めてＷＥＰキーを作成し、作成したＷＥＰキーの端末５０への送信後に通信範囲を元に戻している。従って、端末５０の所有者は、アクセスポイント２０に触れることなくＷＥＰキーの設定を行なうことが可能となり、簡便かつ衛生的である。

【００５３】

第１実施例の暗号鍵設定システムＬＨ１では、アクセスポイント２０が、ＷＥＰキーの設定に併せて端末５０側のＭＡＣアドレスを登録し、登録端末５０，６０についてのみ無線ＬＡＮへの接続を許容する。これにより、非登録端末７０による無線ＬＡＮへの接続を簡便な手法で防止することができる。また、非登録端末７０がＬＡＮ上の登録端末５０，６０やアクセスポイント２０に侵入してＷＥＰキーのデータ等の各種のデータを取得することを未然に防止することができる。

【００５４】

上記第１実施例において、通信範囲を狭める期間としては、（ａ）登録ボタン１２７が押されている間、（ｂ）登録ボタン１２７を押してからＭＡＣアドレスおよびＷＥＰキーが登録されるまでの間、（ｃ）登録ボタン１２７を押してからもう一度押すまでの間等が考えられる。また、通信範囲を狭めるトリガーとして、前記登録ボタン１２７によらずに、アクセスポイント２０が端末５０から加入指示を表わすデータを受信したときとしてもよい。この場合は、該端末５０がセキュリティ通信エリアＭＲ１内にあることを、通信の応答時間で判別することも可能である。

【００５５】

Ｂ．第２実施例（暗号鍵設定システムＬＨ２）：

次に、第２実施例について説明する。第１実施例では、ＷＥＰキーのデータが乗った電波が傍受されることを、ＷＥＰキーの設定の際に通信範囲を一時的に狭めるというソフト的な手法で防止した。これに対し、第２実施例の暗号鍵設定システムＬＨ２では、ＷＥＰキーのデータが乗った電波が傍受されることを、「ア

クセスポイント２０および端末５０を覆うシールド箱９５」というハード的な手法で実現する。

【００５６】

図６は本発明の第２実施例である暗号鍵設定システムＬＨ２を実現する装置構成を示す説明図である。アクセスポイント２０および端末５０，６０，７０は、第１実施例とほぼ同様の構成を備え、このアクセスポイント２０によって第１実施例と同様の無線通信エリアＡＲ１が形成されている。図６に示すように、アクセスポイント２０および端末５０は、敷板９６の上に配置されている。この敷板９６には、アクセスポイント２０，端末５０を包摂可能な中空部を有するシールド箱９５が覆い被せられている。シールド箱９５および敷板９６は鉄等の金属で形成されている。

【００５７】

第２実施例では、ＷＥＰキーの設定を以下の手順で行なう。まず、無線ＬＡＮへの加入を希望する者は、アクセスポイント２０の設置場所に行き、自己の所有する端末５０とアクセスポイント２０を敷板９６の上に配置する。このとき、敷板９６の上には予めアクセスポイント２０が配置されていることとしても差し支えない。次に、無線ＬＡＮへの加入を希望する者は、端末５０を操作して無線ＬＡＮに加入する旨の指示を行なった後、敷板９６にシールド箱９５を被せる。アクセスポイント２０は、端末５０から加入指示を表わすデータを受信し、該受信から所定時間（例えば、シールド箱９５を被せるのに要する時間）の経過後に、第１実施例と同様のＭＡＣアドレスの登録処理やＷＥＰキーの設定処理（ステップＳ１００，ステップＳ２３０，～ステップＳ２６０，ステップＳ２８０，ステップＳ１１０の各処理）を行なう。これにより、アクセスポイント２０側での端末５０に関するＭＡＣアドレスの登録が完了し、アクセスポイント２０で作成されたＷＥＰキーのデータが端末５０に送信されて端末５０へのＷＥＰキーの設定が完了する。

【００５８】

以上説明した第２実施例の暗号鍵設定システムＬＨ２では、ＷＥＰキーの設定の際、ＷＥＰキーのデータをやり取りする端末５０およびアクセスポイント２０

がシールド箱９５によって遮蔽される。このため、ＷＥＰキーデータを乗せた電波が傍受されることを確実に防止することができる。例えば、図６において、アクセスポイント２０から端末５０にＷＥＰキーデータが送信された場合に、ＷＥＰキーデータを乗せた電波は、シールド箱９５を通り抜けることができないので（矢印Ｑ２を参照）、無線通信エリアＡＲ１内の登録端末６０や非登録端末７０に受信されてしまうことがない。また、無線通信エリアＡＲ１内の登録端末６０や非登録端末７０が、ＷＥＰキーデータが乗った電波を傍受しようとした場合であっても、電波はシールド箱９５を通り抜けることができないので（矢印Ｑ３を参照）、ＷＥＰキーデータが乗った電波をキャッチすることができない。従って、ＷＥＰキーデータが無線で送信される場合であっても、ＷＥＰキーデータの漏洩を防止することが可能となり、セキュリティレベルの高い無線ＬＡＮを実現することができる。

【００５９】

Ｃ．変形例：

以上本発明の実施の形態を実施例に基づいて説明したが、本発明はこうした実施例に何等限定されるものではなく、本発明の要旨を逸脱しない範囲内において種々なる様態で実施し得ることは勿論である。

【００６０】

例えば、上記実施例では、アクセスポイント２０に外部アンテナを有線で接続し、外部アンテナと端末５０との無線での通信によってＭＡＣアドレスの登録やＷＥＰキーの設定を行なう構成としても差し支えない。こうすれば、アクセスポイント２０の設置場所の自由度を高めることができる。例えば、店内の隅に外部アンテナを設置して外部アンテナの近辺をＷＥＰキーの設定場所としつつ、店内の中央にアクセスポイント２０を設置して無線通信エリアを店内の全体に広く確保することができる。

【００６１】

上記実施例では、端末とアクセスポイントとの間でやりとりされるデータの内容を暗号化する技術としてＷＥＰを用いたが、ＷＥＰ以外の他の暗号化技術を用いても差し支えない。例えば、公開鍵暗号方式（データの暗号化と暗号化された

データの復号化とで異なる暗号鍵を使用する方式）の暗号化技術を用いてもよい。また、ＷＥＰよりも強度の高い暗号化技術であるＷＰＡ（Ｗｉ－Ｆｉ　Ｐｒｏｔｅｃｔｅｄ　Ａｃｃｅｓｓ）を用いることも考えることができる。

【００６２】

また、上記実施例では、ＷＥＰキーの設定中における無線通信範囲を限定したが、このような無線通信範囲の限定は、ＷＥＰキーのみならず、アクセスポイント２０と端末５０との間のやり取りによって設定される他の情報にも適用することができる。例えば、特定の人に対してのみ有料コンテンツを送信するフリースポットでは、アクセスした端末の所有者が特定の人であることを認証するための情報（例えば、端末所有者の氏名，ＩＤやパスワード等）をアクセスポイント２０や端末５０に予め登録する場合がある。こうした個人を認証する情報の登録を、アクセスポイント２０と端末５０との間の無線通信範囲を限定しつつ、無線通信によって行なう構成としてもよい。こうすれば、ＩＤやパスワード等の個人を認証する情報をマニュアルで設定する必要がない。

【図面の簡単な説明】

【図１】　本発明の第１実施例である暗号鍵設定システムＬＨ１を実現するハードウェアの構成を示す説明図である。

【図２】　アクセスポイント２０の構成を示す説明図である。

【図３】　セキュリティデータ設定処理ルーチンを示すフローチャートである。

【図４】　出力値が変更された後の送信機２５における電波の送信可能範囲を、セキュリティ通信エリアＭＲ１として示す説明図である。

【図５】　本発明の第２実施例である暗号鍵設定システムＬＨ２を実現する装置構成を示す説明図である。

【符号の説明】

１１…ＣＰＵ

１２…ＲＯＭ

１３…ＲＡＭ

１４…記憶装置

１５…ディスプレイコントローラ

１６…入出力コントローラ

１７…ＷＡＮポート

１８…無線通信インタフェース

１９…表示ランプ

２０…アクセスポイント

２２…ＬＡＮポート

２５…送信機

２６…受信機

２８…ルータ

５０，６０，７０…端末

５２，６２，７２…無線ＬＡＮアダプタ

９５…シールド箱

９６…敷板

１２７…登録ボタン

ＡＲ１…無線通信エリア

ＣＬ…通信回線

ＩＮ…インターネット

ＬＨ１，ＬＨ２…暗号鍵設定システム

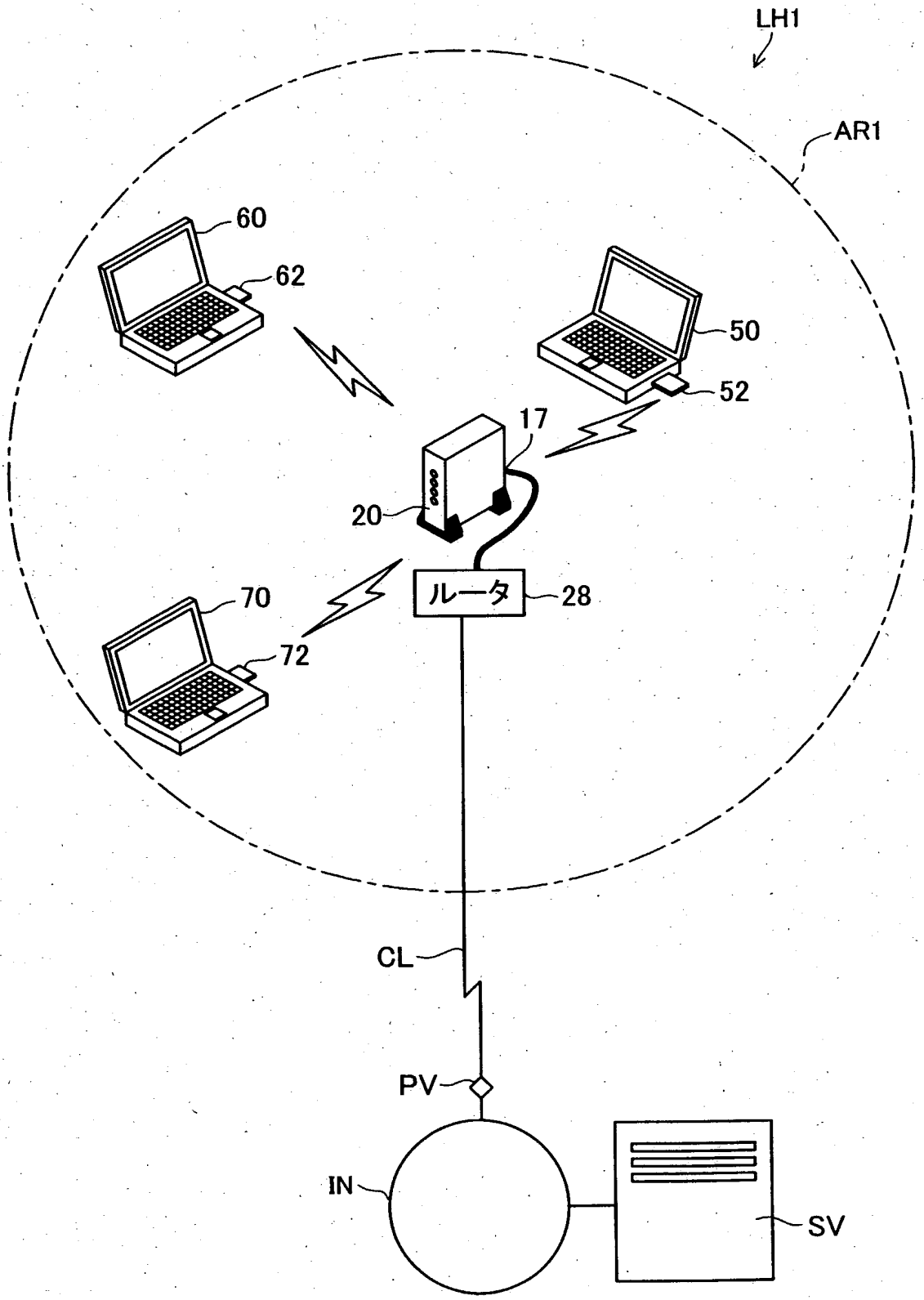
ＭＲ１…セキュリティ通信エリア

ＰＶ…プロバイダ

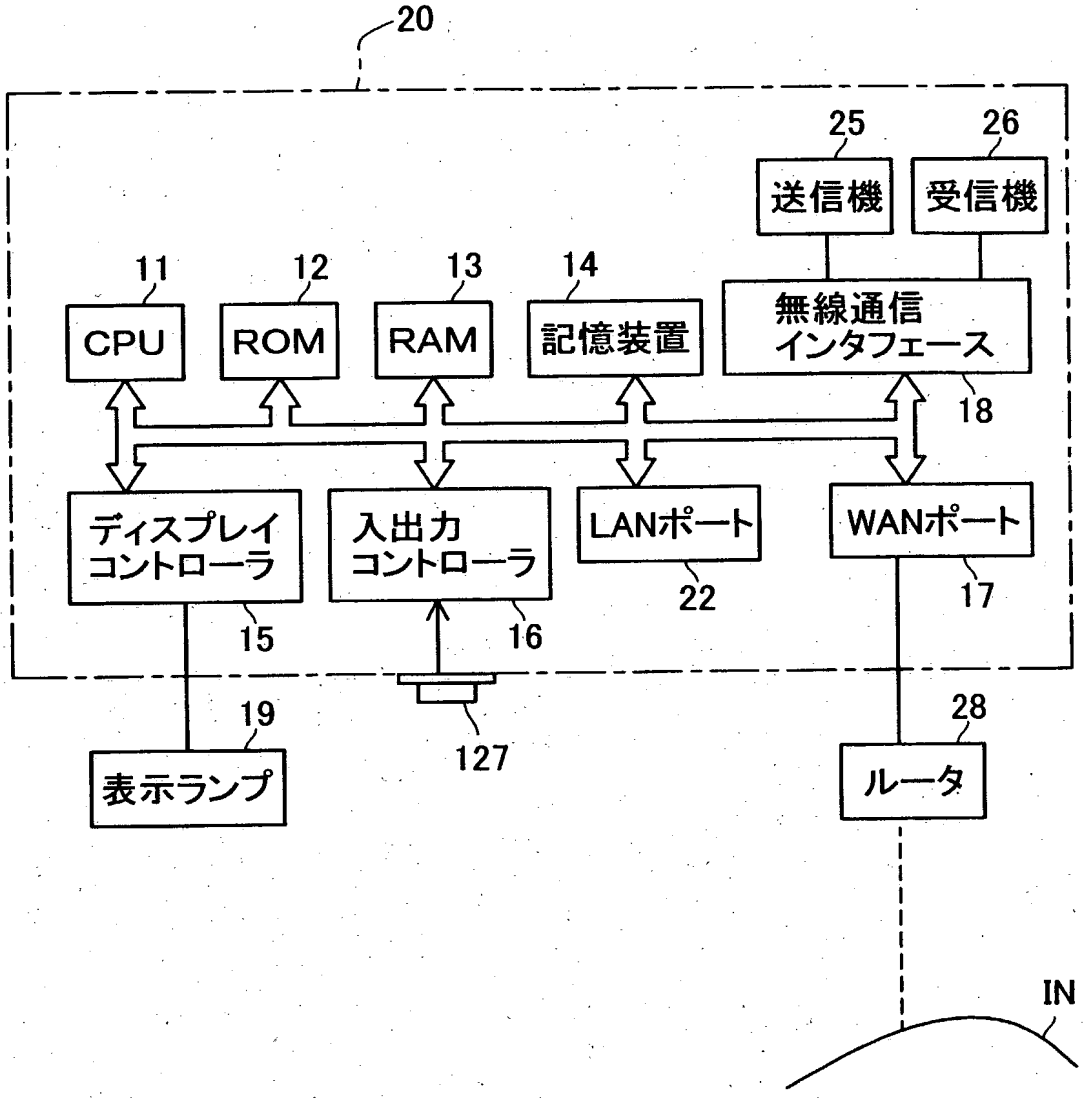
ＳＶ…サーバ

【書類名】　　図面

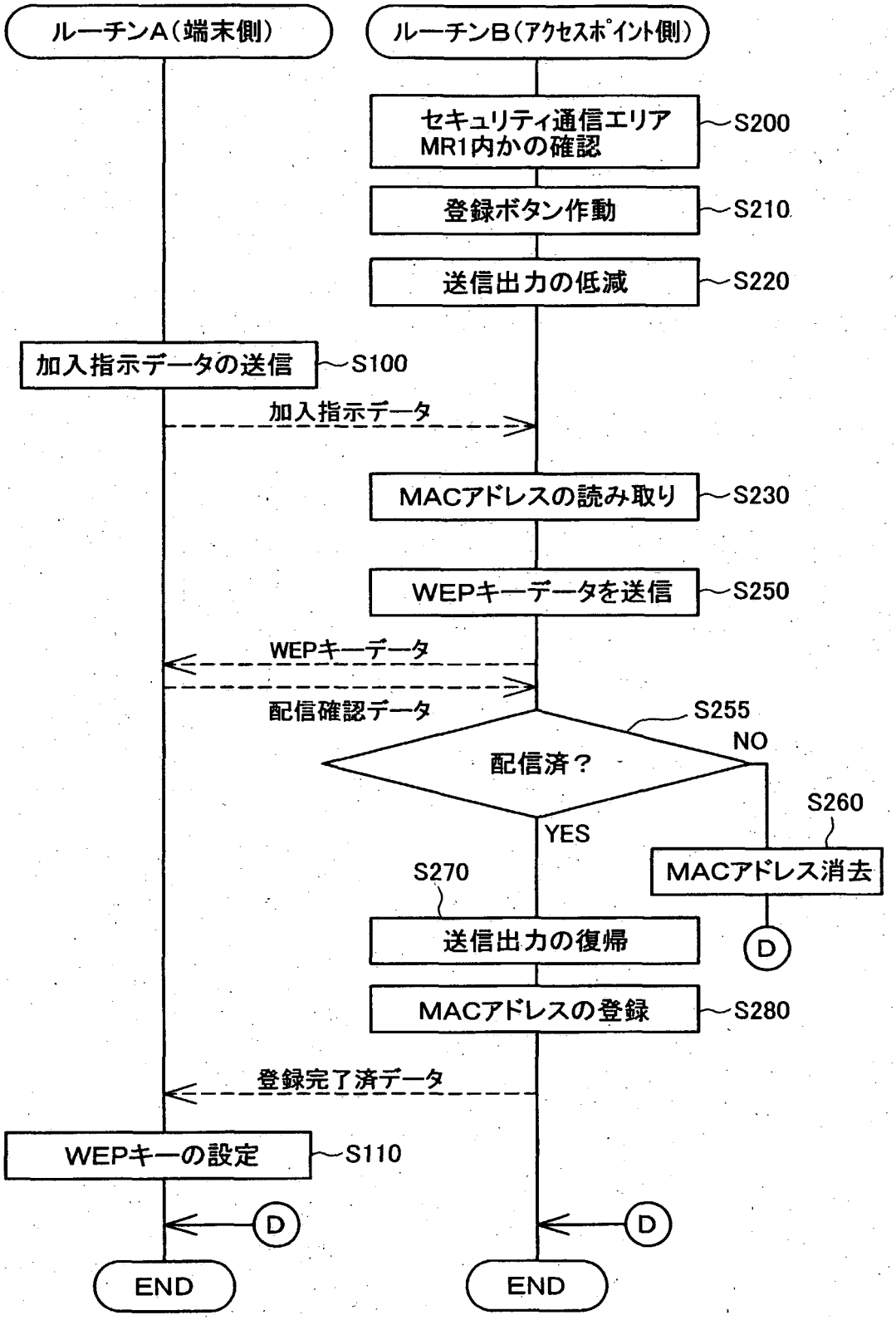
【図１】



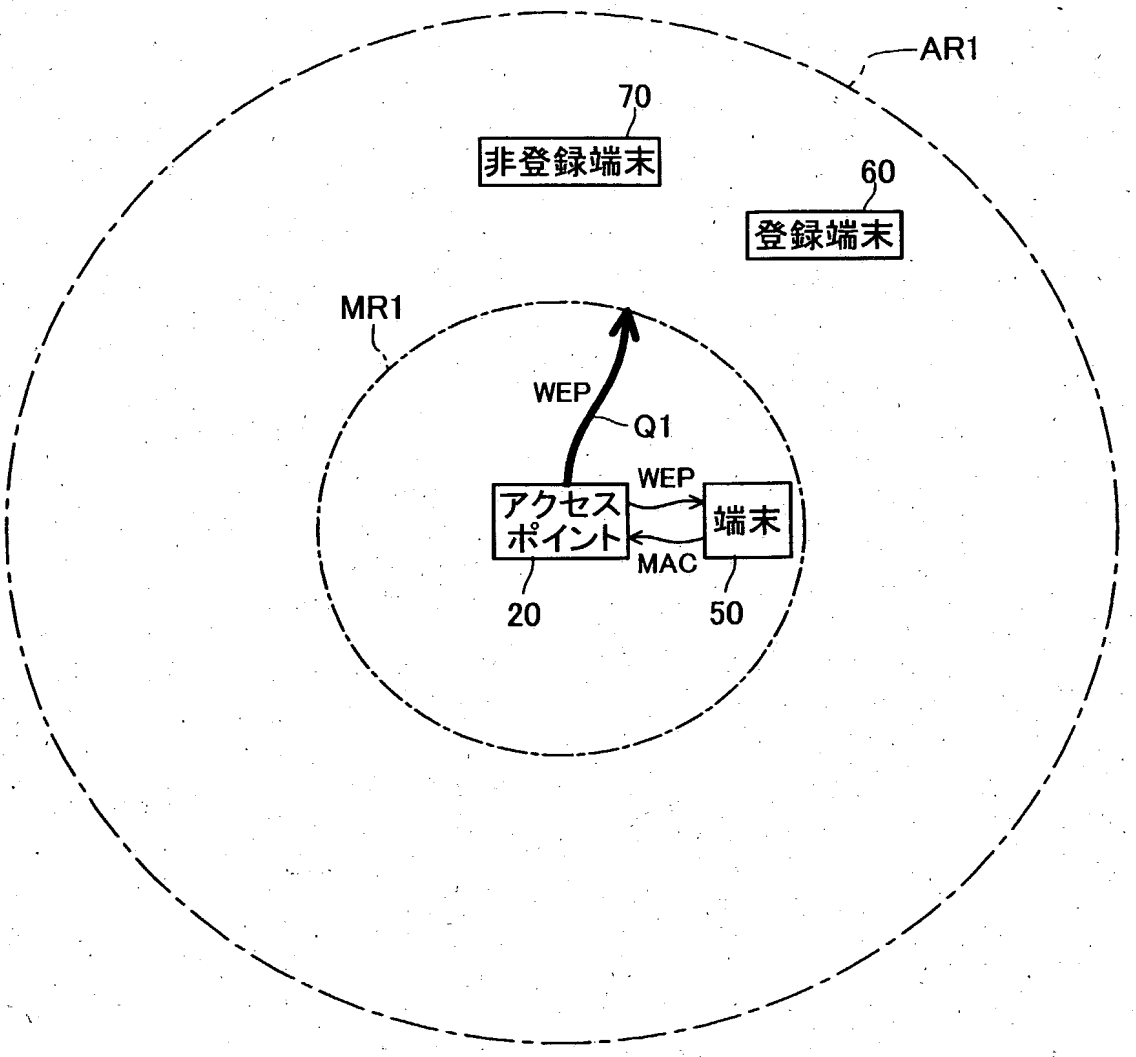
【図２】


20
25
26
送信機
受信機
11
12
13
14
CPU
ROM
RAM
記憶装置
無線通信
インタフェース
18
ディスプレイ
コントローラ
入出力
コントローラ
LANポート
WANポート
22
17
15
16
19
127
28
表示ランプ
ルータ
IN

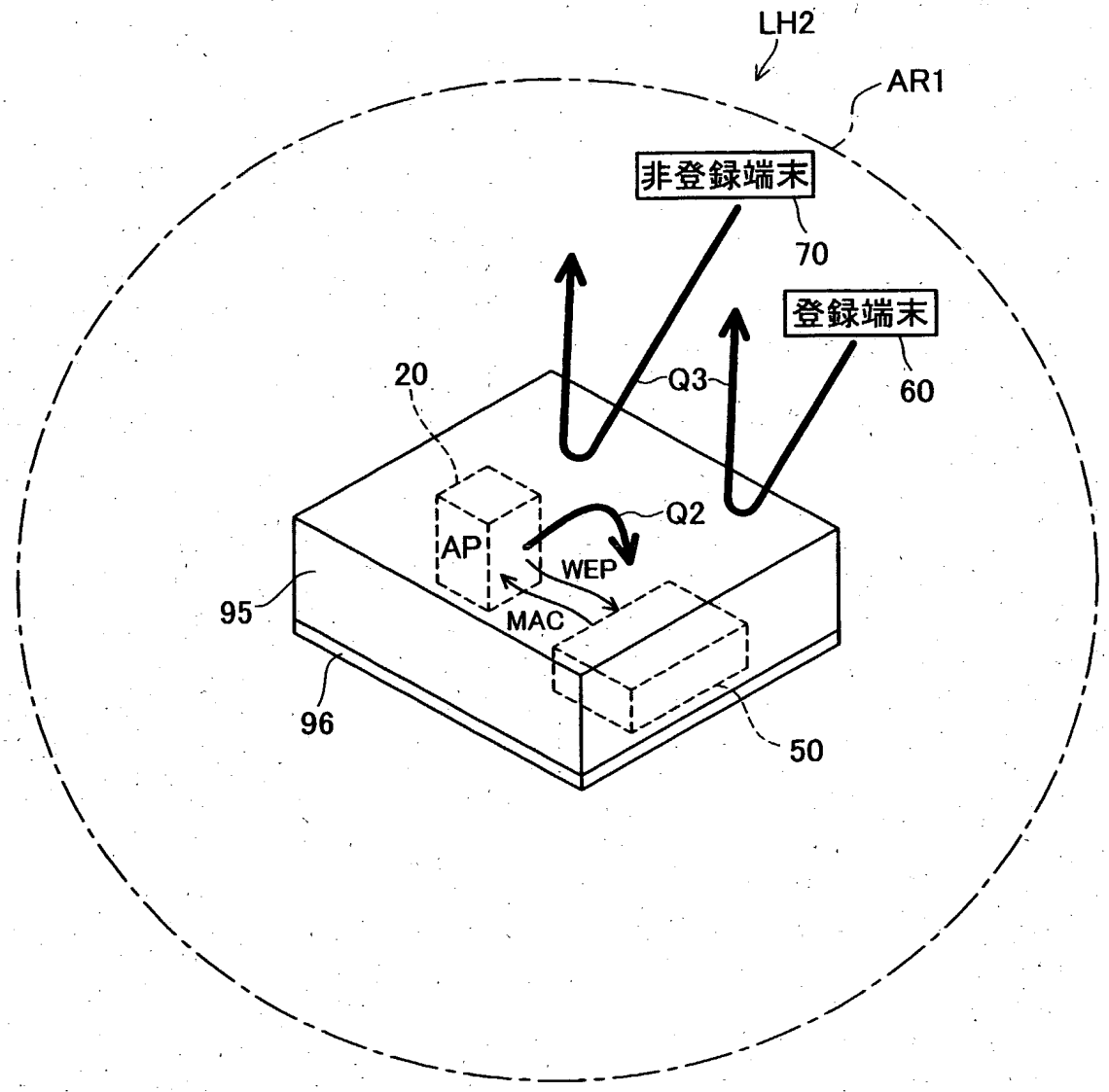
【図３】


ルーチンA（端末側）
ルーチンB（アクセスポイント側）
セキュリティ通信エリア MR1内かの確認
S200
登録ボタン作動
S210
送信出力の低減
S220
加入指示データの送信
S100
加入指示データ
MACアドレスの読み取り
S230
WEPキーデータを送信
S250
WEPキーデータ
配信確認データ
S255
配信済？
NO
YES
S260
MACアドレス消去
S270
送信出力の復帰
D
MACアドレスの登録
S280
登録完了済データ
WEPキーの設定
S110
D
D
END
END

【図４】



【図５】



【書類名】　　要約書

【要約】

【課題】　無線ＬＡＮを利用する端末の新規追加を、暗号鍵を表わすデータの漏洩を防止しつつ、簡便な手法で実現することを目的とする。

【解決手段】　アクセスポイント２０は、登録ボタン１２７の作動により、アクセスポイント２０から送信される電波が届く範囲を、通常の範囲である無線通信エリアＡＲ１から、より狭い範囲であるセキュリティ通信エリアＭＲ１に変更する。この後、アクセスポイント２０は、使用されるＷＥＰキーを端末５０に配信し、配信確認の後、端末５０のＭＡＣアドレスを登録する。端末５０は配信されたＷＥＰキーを自己に設定する。

【選択図】　　図３

出 願 人 履 歴 情 報

識別番号　〔３９００４０１８７〕

１．変更年月日　１９９０年１２月１０日
［変更理由］　新規登録
住　所　愛知県名古屋市中区大須４丁目１１番５０号
氏　名　株式会社メルコ